1. (currently amended) A method for multiplying an elliptic curve point Q(x,y) by a scalar to provide a point kQ, the method comprising the steps of:

a) selecting an elliptic curve of order n over a finite field F such that there exists an endomorphism $\psi$ where $\psi$ (Q) = $\lambda$ (Q) for all point Q (x,y) on the elliptic curve, and $\lambda$ is an integer,

b) establishing a representation of said scalar k as a combination of components $k_i$ and said integer $\lambda$ of the form $k_i = \sum_{i=0}^{i=} k_i \lambda^i$ mod n.

c) combining said representation and said point Q to form a composite representation of a multiple of the form $k_0Q + k_1 \psi (Q) + \ldots$ corresponding to kQ; and

d) computing a value corresponding to said point kQ from said composite representation of kQ.

2. (original) A method according to claim 1 wherein each of said components $k_i$ is shorter than said scalar k.

3. (original) A method according to claim 1 wherein said components $k_i$ are initially selected and subsequently combined to provide said scalar k.

4. (currently amended) A method according to claim 1 wherein said components $k_i$ are selected at random. [representation is of the form $k_i = \sum_{i=0}^{i=} k_i \lambda^i$ mod n where n is the number of points on the elliptic curve].

5. (currently amended) A method according to claim 4 wherein said representation is of the form $k_0 + k_1 \lambda$.

6. (currently amended) A method according to claim 1 wherein said scalar k has a predetermined value and said components $k_0$ and $k_1$ are one half size of said scalar k.

7. (original) A method according to claim 3 wherein said value of said multiple kQ is calculated using simultaneous multiple addition.

8. (original) A method according to claim 7 wherein grouped terms $G_l$ utilized in said simultaneous multiple addition are precomputed.

9. (original) A method according to claim 6 wherein said components $k_i$ are obtained by obtaining short basis vectors $(u_o, u_i)$ of the field F, designating a vector v as (k,0), converting v from a standard, orthonomal basis to the $(u_o, u_i)$ basis, to obtain fractions $f_o f_i$ representative of the vector v, applying said fractions to k to obtain a vector z, calculating an efficient equivalent v` in the composite representation of kQ.

10. (currently amended) A method of generating in an elliptic curve cryptosystem a key pair having a integer k providing a private key and a public key kQ, where Q is a point on the curve,

a) selecting an elliptic curve over a finite filed F such that there exists an endomorphism $\psi$ where $\psi$ (Q) = $\lambda$ Q for all points Q (x,y) on the elliptic curve, $\lambda$ is an integer,

b) establishing a representation of said key k as a combination of components $k_i$ and said integer $\lambda$, <u>of the form $k_i = \sum_{i=0}^{i=} k_i \lambda^i$ mod n where n is the number of points on the elliptic curve,</u>

c) combining said representation and said point Q to form a composite representation of a multiple <u>of the form $k_0Q + k_1 \psi(Q) + \ldots$</u> corresponding to the public key kQ<u>; and</u>

d) computing a value corresponding to said <u>public</u> kQ from said composite representation of kQ.

11. (currently amended) A method according to claim 10 [including a method according to any one of claims 2 to 9] <u>wherein each of said components $k_i$ is shorter than said scalar k</u>.

12. (new) A method according to claim 11 wherein said components $k_i$ are initially selected and subsequently combined to provide said scalar k.

13. (new) A method according to claim 12 said components $k_i$ are selected at random.

14. (new) A method according to claim 13 wherein said representation is of the form $k_0 + k_1 \lambda$.

15. (new) A method according to claim 10 wherein said scalar k has a predetermined value and said components $k_0$ and $k_1$ are selected to be one half the size of said scalar k.

16. (new) A method according to claim 12 wherein said value of said multiple kQ is calculated using simultaneous multiple addition.

17. (new) A method according to claim 16 wherein grouped terms $G_I$ utilized in said simultaneous multiple addition are precomputed.

18. (new) A method according to claim 15 wherein said components $k_i$ are obtained by obtaining short basis vectors ($u_o$, $u_i$) of the field F, designating a vector v as (k,0), converting v from a standard, orthonomal basis to the ($u_o$, $u_i$) basis, to obtain fractions $f_0 f_i$ representative of the vector v, applying said fractions to k to obtain a vector z, calculating an efficient equivalent v` in the composite representation of kQ.